第 36 卷 第 4 期
2013 年 4 月

计 算 机 学 报
CHINESE JOURNAL OF COMPUTERS

Vol. 36 No. 4
Apr. 2013

L_3^* 中逻辑公式的范式表示及对称逻辑公式的构造方法

王庆平

(江西财经大学统计学院 南昌 330013)
(陕西师范大学数学与信息科学学院 西安 710062)

摘 要 将符号化计算树逻辑中 Boole 函数的 Shannon 展开式做了推广,研究了三值逻辑系统 L_3^* 中由公式导出的三值 R_0 函数的展开式,给出了 L_3^* 中逻辑公式的准析取范式和准合取范式表示.研究了 n 元三值 R_0 函数以及 n 元逻辑公式逻辑等价类的计数问题.在此基础上,给出了 L_3^* 中对称逻辑公式的构造方法.

关键词 Shannon 展开式;三值 R_0 函数;对称逻辑公式;范式表示;计数问题
中图法分类号 TP301 **DOI 号** 10.3724/SP.J.1016.2013.00851

The Normal Form of Logic Formulae and Construction Method of Symmetrical Logic Formulae in L_3^*

WANG Qing-Ping

(*School of Statistics, Jiangxi University of Finance and Economics, Nanchang* 330013)
(*College of Mathematics and Information Science, Shaanxi Normal University, Xi'an* 710062)

Abstract Shannon expansion of Boole function in symbolic computation tree logic is generalized. In three-valued logic system L_3^*, the expansions of symmetric three-valued R_0 function which are induced by logical formulae are studied, and the quasi disjunctive normal form and quasi conjunctive normal form of logical formulae are given. The counting problems of n-ary three-valued R_0 functions and n-ary logical formulae are studied. Then the construction method of symmetrical logic formulae in L_3^* is given.

Keywords Shannon expansion; three-valued R_0 function; symmetrical logic formulae; normal form; counting problem

1 引 言

模型检验(Model Checking)技术自提出以来已在包括航空航天、电子商务、通信技术乃至医疗系统等各个领域取得了成功的应用,所以近年来得到了迅速的发展[1-7]. 所谓模型是指包含有状态集、状态转移关系以及与一组原子命题相联系的迁移系统(Transition System,TS),而模型检验的任务就在于通过某种自动化的方法检验一个 TS 是否满足预定的规范(Specification). 这里的规范通常用具有足够强的表述功能的逻辑公式 φ 来表示,φ 经常取为计算树逻辑(Computing Tree Logic)中的公式,简称为 CTL 公式. 模型检验技术虽然是自动化的,但对于复杂的规范往往会出现计算复杂性不断增加乃至出现状态爆炸的情况. 为了简化检验过程,在计算树逻辑的模型检验中,文献[1]给出了开关函数(switching functions)的概念,并借助于 Shannon 展开式将状态(states)和状态之间的转移关系符号化,实现了符号化的计算树逻辑的模型检验.

收稿日期:2011-04-25;最终修改稿收到日期:2012-05-27. 本课题得到国家自然科学基金(11171200,61005046,61103133)、教育部高等学校博士学科点专项科研资金(20100202120012)资助. 王庆平,男,1979 年生,博士研究生,讲师,主要研究方向为模糊逻辑、不确定性推理. E-mail: lc_wqp@163.com.

Boole 函数是数理逻辑中的重要概念，而且 Boole 函数也是研究数字电路、密码学和密码技术的重要工具. 不同的密码系统对 Boole 函数有不同的要求，某一性质保证某一方面的安全性. 但并不是一个函数满足的性质越多越好，因为满足的性质越多，函数类越小，函数的选择范围将缩小，从而失去灵活性，反而降低安全性. 所以，一个函数类的计数问题是一个重要的研究课题. 文献[8]系统地研究了密码学中的布尔函数，其中对称布尔函数是一类重要的布尔函数，关于对称布尔函数的研究取得了丰富的成果[9-10]. 文献[11]研究了三值逻辑系统 L_3^* 中的对称逻辑公式，给出了由逻辑公式导出的三值 R_0 函数的概念. 与 Boole 函数不同的是：n 元 Boole 函数共有 2^{2^n} 个；而 n 元三值 R_0 函数的个数却少于 3^{3^n} 个，例如 $\bar{g}(x_1,\cdots,x_n)=\dfrac{1}{2}$ 就不是三值 R_0 函数. 本文借助模型检验中 Boole 函数 Shannon 展开式的巧妙思想，给出三值 R_0 函数的展开式以及三值 R_0 函数的构造方法，并证明 n 元三值 R_0 函数共有 $2^{2^n}\times 3^{3^n-2^n}$ 个. 在此基础上，给出了 L_3^* 逻辑系统中逻辑公式的准析取范式和准合取范式表示，从而为解决逻辑等价类的计数问题奠定基础，特别是给出了 L_3^* 逻辑系统中对称逻辑公式构造方法，并解决相应的计数问题.

2 预备知识

定义 1[12]. 设 $S=\{p_1,p_2,\cdots\}$，作 $F(S)$ 如下：

(1) $p_1,p_2,\cdots\in F(S)$；

(2) 若 $A,B\in F(S)$，则 $\neg A, A\to B\in F(S)$；

(3) $F(S)$ 中的元都可通过(1)与(2)而得到.

$F(S)$ 是 S 生成的 $(\neg,\to)$ 型自由代数，S 中的元叫原子命题、命题变元或原子公式，$F(S)$ 中的元叫命题或合式公式，简称公式.

注 1. 在定义 1 中并未用到逻辑连接词 $\vee$ 与 $\wedge$，其实它们都可以用 $\neg$ 与 $\to$ 表达. 规定：$A\vee B$ 与 $A\wedge B$ 分别是 $\neg A\to B$，$\neg(A\to\neg B)$ 的简写.

定义 2[12]. 设 $v: F(S)\to\{0,1\}$ 是映射，这里 $\{0,1\}$ 是 Boole 代数，若 v 是 $(\neg,\to)$ 型同态，即

$$v(\neg A)=\neg v(A),\ v(A\to B)=v(A)\to v(B),$$

则称 v 为 $F(S)$ 的赋值，$v(A)$ 也叫公式 A 的赋值，$F(S)$ 中全体赋值之集记作 Ω.

定义 3[12]. 设 $A,B\in F(S)$.

(1) 如果对每个 $v\in\Omega$，均有 $v(A)=1$，则称 A 为重言式，记作 $\models A$；如果对每个 $v\in\Omega$，均有 $v(A)=0$，则称 A 为矛盾式.

(2) 如果对每个 $v\in\Omega$，均有 $v(A)=v(B)$，则称 A 与 B 逻辑等价，记作 $A\approx B$.

定义 4[12]. 函数 $f:\{0,1\}^n\to\{0,1\}$ 叫 n 元 Boole 函数($n\in N$).

定义 5[12]. 设 $A(p_1,\cdots,p_n)$ 是含有 n 个命题变元的合式公式，它由 $p_1,\cdots,p_n$ 通过逻辑连接词 $\neg$、$\to$、$\vee$ 与 $\wedge$ 连接而成. 设 $(x_1,\cdots,x_n)\in\{0,1\}^n$，分别用 $x_1,\cdots,x_n$ 取代 $A(p_1,\cdots,p_n)$ 中的 $p_1,\cdots,p_n$，并按 $\neg 0=1$，$\neg 1=0$，$a\to b=0$ 当且仅当 $a=1,b=0$，$a\vee b=\max\{a,b\}$，$a\wedge b=\min\{a,b\}$ 理解 $\neg$，$\to$，$\vee$ 与 $\wedge$，则得一 n 元函数，记作 $\overline{A}(x_1,\cdots,x_n)$ 叫作公式 A 导出的 Boole 函数.

命题 1[12]. 每个 Boole 函数都可由某公式导出.

定义 6[12]. 设 $A(p_1,\cdots,p_n)\in F(S)$，则分别当 A 具有形式

$(Q_{11}\wedge\cdots\wedge Q_{1n})\vee\cdots\vee(Q_{m1}\wedge\cdots\wedge Q_{mn})$ 或

$(Q_{11}\vee\cdots\vee Q_{1n})\wedge\cdots\wedge(Q_{m1}\vee\cdots\vee Q_{mn})$

时，称 A 为析取范式或合取范式，这里 $Q_{ij}=p_j$ 或 $Q_{ij}=\neg p_j$ ($j=1,\cdots,n$; $i=1,\cdots,m$).

注 2. 由原子公式或其否定通过析(合)取连接词连接而成的公式叫简单析(合)取式. 如 $p_1\vee p_2\vee\neg p_3$ 是简单析取式，$\neg p_1\wedge p_2$ 是简单合取式. 简单析(合)取式既可以看作是析取范式，又可以看做合取范式.

定义 7[1]. 设 $f(x_1,\cdots,x_n)$ 为 n 元 Boole 函数，称下式为 Shannon 展开式：

$$f(x_1,x_2,\cdots,x_n)=(\neg x_1\wedge f(0,x_2,\cdots,x_n))\vee (x_1\wedge f(1,x_2,\cdots,x_n)).$$

下面，我们给出 Shannon 展开式的推广形式.

命题 2. 设 $f(x_1,\cdots,x_n)$ 为 n 元 Boole 函数，约定 $x_k^0=\neg x_k$，$x_k^1=x_k$ ($k=1,2$)，则

$$f(x_1,x_2,x_3,\cdots,x_n)=\bigvee\{x_1^{\alpha_1}\wedge x_2^{\alpha_2}\wedge f(\alpha_1,\alpha_2,x_3,\cdots,x_n):(\alpha_1,\alpha_2)\in\{0,1\}^2\}.$$

证明. 由 Shannon 展开式可得

$$f(x_1,x_2,x_3,\cdots,x_n)=(\neg x_1\wedge f(0,x_2,x_3,\cdots,x_n))\vee (x_1\wedge f(1,x_2,x_3,\cdots,x_n)) \quad (1)$$

又

$$f(0,x_2,x_3,\cdots,x_n)=(\neg x_2\wedge f(0,0,x_3,\cdots,x_n))\vee (x_2\wedge f(0,1,x_3,\cdots,x_n)),$$

$$f(1,x_2,x_3,\cdots,x_n)=(\neg x_2\wedge f(1,0,x_3,\cdots,x_n))\vee (x_2\wedge f(1,1,x_3,\cdots,x_n)),$$

代入式(1)，整理得

$$f(x_1,x_2,x_3,\cdots,x_n)=(\neg x_1\wedge\neg x_2\wedge f(0,0,x_3,\cdots,x_n))\vee (\neg x_1\wedge x_2\wedge f(0,1,x_3,\cdots,x_n))\vee (x_1\wedge\neg x_2\wedge f(1,0,x_3,\cdots,x_n))\vee (x_1\wedge x_2\wedge f(1,1,x_3,\cdots,x_n)) =\vee\{x_1^{\alpha_1}\wedge x_2^{\alpha_2}\wedge f(\alpha_1,\alpha_2,x_3,\cdots,x_n):(\alpha_1,\alpha_2)\in\{0,1\}^2\}.$$

证毕.

更一般地，由命题 2 的推广思路可进一步得出 Boole 函数的析取范式如下.

推论 1. 设 $f(x_1,\cdots,x_n)$为 n 元 Boole 函数，约定 $x_k^0=\neg x_k$，$x_k^1=x_k(k=1,2,\cdots,n)$，则

$$f(x_1,\cdots,x_n)=\vee\{x_1^{\alpha_1}\wedge\cdots\wedge x_n^{\alpha_n}\wedge f(\alpha_1,\cdots,\alpha_n):(\alpha_1,\cdots,\alpha_n)\in\{0,1\}^n\} =\vee\{x_1^{\alpha_1}\wedge\cdots\wedge x_n^{\alpha_n}:(\alpha_1,\cdots,\alpha_n)\in f^{-1}(1)\}.$$

注 3. 若 $f^{-1}(1)=\varnothing$，即 $f(x_1,\cdots,x_n)=0$. 这时，可令 $f(x_1,\cdots,x_n)=x_1\wedge\neg x_1$.

下面，我们再给出 Shannon 展开式的对偶形式及其推广.

命题 3. 设 $f(x_1,\cdots,x_n)$为 n 元 Boole 函数，约定 $x_k^0=x_k$，$x_k^1=\neg x_k(k=1,2)$，则

(1) $f(x_1,x_2,\cdots,x_n)=(x_1\vee f(0,x_2,\cdots,x_n))\wedge(\neg x_1\vee f(1,x_2,\cdots,x_n))$.

(2) $f(x_1,x_2,x_3,\cdots,x_n)=\wedge\{x_1^{\beta_1}\vee x_2^{\beta_2}\vee f(\beta_1,\beta_2,x_3,\cdots,x_n):(\beta_1,\beta_2)\in\{0,1\}^2\}$.

证明.

(1) $x_1=0$ 时，$(x_1\vee f(0,x_2,\cdots,x_n))\wedge(\neg x_1\vee f(1,x_2,\cdots,x_n))=(0\vee f(0,x_2,\cdots,x_n))\wedge(1\vee f(1,x_2,\cdots,x_n))=f(0,x_2,\cdots,x_n)\wedge 1=f(0,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)$.

$x_1=1$ 时，$(x_1\vee f(0,x_2,\cdots,x_n))\wedge(\neg x_1\vee f(1,x_2,\cdots,x_n))=(1\vee f(0,x_2,\cdots,x_n))\wedge(0\vee f(1,x_2,\cdots,x_n))=1\wedge f(1,x_2,\cdots,x_n)=f(1,x_2,\cdots,x_n)=f(x_1,x_2,\cdots,x_n)$.

(2) 由(1)可得

$$f(x_1,x_2,x_3,\cdots,x_n)=(x_1\vee f(0,x_2,x_3,\cdots,x_n))\wedge(\neg x_1\vee f(1,x_2,x_3,\cdots,x_n)) \quad (2)$$

又

$$f(0,x_2,x_3,\cdots,x_n)=(x_2\vee f(0,0,x_3,\cdots,x_n))\wedge(\neg x_2\vee f(0,1,x_3,\cdots,x_n)),$$
$$f(1,x_2,x_3,\cdots,x_n)=(x_2\vee f(1,0,x_3,\cdots,x_n))\wedge(\neg x_2\vee f(1,1,x_3,\cdots,x_n)),$$

代入式(2)，整理得

$$f(x_1,x_2,x_3,\cdots,x_n)=(x_1\vee x_2\vee f(0,0,x_3,\cdots,x_n))\wedge (x_1\vee\neg x_2\vee f(0,1,x_3,\cdots,x_n))\wedge (\neg x_1\vee x_2\vee f(1,0,x_3,\cdots,x_n))\wedge (\neg x_1\vee\neg x_2\vee f(1,1,x_3,\cdots,x_n)) =\wedge\{x_1^{\beta_1}\vee x_2^{\beta_2}\vee f(\beta_1,\beta_2,x_3,\cdots,x_n):(\beta_1,\beta_2)\in\{0,1\}^2\}.$$

证毕.

基于命题 3 中的方法可得出 Boole 函数的合取范式如下.

推论 2. 设 $f(x_1,\cdots,x_n)$为 n 元 Boole 函数，约定 $x_k^0=x_k$，$x_k^1=\neg x_k(k=1,2,\cdots,n)$，则

$$f(x_1,\cdots,x_n)=\wedge\{x_1^{\beta_1}\vee\cdots\vee x_n^{\beta_n}\vee f(\beta_1,\cdots,\beta_n):(\beta_1,\cdots,\beta_n)\in\{0,1\}^n\} =\wedge\{x_1^{\beta_1}\vee\cdots\vee x_n^{\beta_n}:(\beta_1,\cdots,\beta_n)\in f^{-1}(0)\}.$$

注 4. 若 $f^{-1}(0)=\varnothing$，即 $f(x_1,\cdots,x_n)=1$. 这时，可令 $f(x_1,\cdots,x_n)=x_1\vee\neg x_1$.

命题 4[12]**.** 每个公式都逻辑等价于一个析取范式(或合取范式).

文献[12]给出了命题 4 的构造性证明，下面根据 Shannon 展开式及其推广形式给出一种新的证明方法.

证明. 仅证析取范式的情形(合取范式的情形是类似的).

$\forall A\in F(S)$，不妨设A中含有n个原子命题$p_1,\cdots,p_n$，则 A 导出一个 n 元 Boole 函数 $\overline{A}(x_1,\cdots,x_n)$.

若 A 不是矛盾式，则 $\overline{A}^{-1}(1)\neq\varnothing$. 由推论 1 可知，约定 $x_k^0=\neg x_k$，$x_k^1=x_k(k=1,2,\cdots,n)$，则

$$\overline{A}(x_1,\cdots,x_n)=\vee\{x_1^{\alpha_1}\wedge\cdots\wedge x_n^{\alpha_n}:(\alpha_1,\cdots,\alpha_n)\in\overline{A}^{-1}(1)\}.$$

这时，约定 $p_k^0=\neg p_k$，$p_k^1=p_k(k=1,2,\cdots,n)$，令 $B=\vee\{p_1^{\alpha_1}\wedge\cdots\wedge p_n^{\alpha_n}:(\alpha_1,\cdots,\alpha_n)\in\overline{A}^{-1}(1)\}$，则 B 导出的 n 元 Boole 函数 $\overline{B}(x_1,\cdots,x_n)=\overline{A}(x_1,\cdots,x_n)$. 所以 $A\approx B$，且 B 是析取范式.

若 A 是矛盾式，则 $\overline{A}(x_1,\cdots,x_n)=0$. 由注 3 可令 $\overline{A}(x_1,\cdots,x_n)=x_1\wedge\neg x_1$，这时取公式 $B=p_1\wedge\neg p_1$，则 $\overline{B}(x_1)=\overline{A}(x_1,\cdots,x_n)$. 所以 $A\approx B$，且 B 是简单合取式，可看作析取范式.　　证毕.

3 L_3^* 中的逻辑公式的范式表示及计数问题

在经典逻辑系统中，每一个 n 元 Boole 函数 f：$\{0,1\}^n\to\{0,1\}$都可由某合式公式导出. 然而，在三值逻辑系统中，每一个 n 元三值函数$\bar{g}$：$\left\{0,\frac{1}{2},1\right\}^n\to$

$\left\{0,\frac{1}{2},1\right\}$却不一定能由某个合式公式导出. 例如, $\bar{g}(x_1,\cdots,x_n)=\frac{1}{2}$就不能由合式公式导出,因为当 $x_1,\cdots,x_n$只取$\{0,1\}$两个值时,使用连接词$\neg$,$\rightarrow$,$\vee$与$\wedge$只能得到0或1,不可能得出$\frac{1}{2}$. 因此,在三值逻辑系统中,由n元公式导出的n元三值函数的形式要比n元Boole函数复杂得多. 下面,本文在三值命题演算系统L_3^*中研究逻辑公式与三值函数的关系.

定义8[12]. 设$S=\{p_1,p_2,\cdots\}$,$F(S)$是由S生成的$(\neg,\vee,\rightarrow)$型自由代数,称$F(S)$中的元为系统L_3^*中的公式(或命题),称S中的元为系统L_3^*中的原子公式(或原子命题).

注5. 在L_3^*中,$A\vee B$不再是$\neg A\rightarrow B$的简写,$\vee$是独立的连接词; $A\wedge B$是$\neg(\neg A\vee\neg B)$的简写.

定义9[12]. 设$v:F(S)\rightarrow\left\{0,\frac{1}{2},1\right\}$是映射,这里$\left\{0,\frac{1}{2},1\right\}$是三值$R_0$-代数,若$v$是$(\neg,\vee,\rightarrow)$型同态,即

$$v(\neg A)=\neg v(A),v(A\vee B)=v(A)\vee v(B)=\max\{v(A),v(B)\},$$
$$v(A\rightarrow B)=v(A)\rightarrow v(B)=R_0(v(A),v(B)),$$

则称v为$F(S)$在三值R_0-代数$\left\{0,\frac{1}{2},1\right\}$中的赋值,简称$v$为赋值. $F(S)$中全体赋值之集记作$\bar{\Omega}$.

在L_3^*中,重言式、矛盾式、逻辑等价以及由公式A导出的函数的定义与经典逻辑系统中的定义是一致的,这里不再赘述.

定义10. 若函数$g:\left\{0,\frac{1}{2},1\right\}^n\rightarrow\left\{0,\frac{1}{2},1\right\}$可由$L_3^*$中的某个$n$元公式导出,则称$g$为$n$元三值$R_0$函数$(n\in N)$.

注6. n元三值R_0函数$g(x_1,\cdots,x_n)$是全体n元三值函数$g:\left\{0,\frac{1}{2},1\right\}^n\rightarrow\left\{0,\frac{1}{2},1\right\}$的一部分. 全体$n$元三值函数共$3^{3^n}$个,在这$3^{3^n}$个函数中,有些不能由合式公式导出.

例1. 设$A_1=\neg(\neg p_1\rightarrow p_1)$,$B_1=\neg(p_1\rightarrow\neg p_1)$,$C_1=(p_1\rightarrow\neg p_1)\wedge(\neg p_1\rightarrow p_1)$,$C_1'=(p_1\rightarrow\neg p_1)\wedge(\neg p_1\rightarrow p_1)\wedge p_1$,令$D_1=\neg(A_1\vee B_1\vee C_1)$,$D_2=B_1$,$D_3=C_1'$,$D_4=B_1\vee C_1'$,$D_5=C_1$,$D_6=B_1\vee C_1$,$D_7=A_1$,$D_8=A_1\vee B_1$,$D_9=A_1\vee C_1'$,$D_{10}=A_1\vee B_1\vee C_1'$,$D_{11}=A_1\vee C_1$,$D_{12}=A_1\vee B_1\vee C_1$,则表1给出由$D_i(i=1,2,\cdots,12)$这12个公式导出的一元三值$R_0$函数.

表1 一元三值R_0函数表

p_1的值	三值函数											
	$\bar{D}_1$	$\bar{D}_2$	$\bar{D}_3$	$\bar{D}_4$	$\bar{D}_5$	$\bar{D}_6$	$\bar{D}_7$	$\bar{D}_8$	$\bar{D}_9$	$\bar{D}_{10}$	$\bar{D}_{11}$	$\bar{D}_{12}$
0	0	0	0	0	0	0	1	1	1	1	1	1
1	0	1	0	1	0	1	0	1	0	1	0	1
$\frac{1}{2}$	0	0	$\frac{1}{2}$	$\frac{1}{2}$	1	1	0	0	$\frac{1}{2}$	$\frac{1}{2}$	1	1

由表1可以看出: 当p_1赋值为0,1时,$\bar{D}_k(k=1,2,\cdots,12)$的值只能为0,1; 当$p_1$赋值为$\frac{1}{2}$时,$\bar{D}_k(k=1,2,\cdots,12)$的值可为3个值$0,1,\frac{1}{2}$. 从而可知,所有的一元三值$R_0$函数至多有$2\times2\times3=12$个,而例1中所给的12个公式恰好导出了12个不同的一元三值R_0函数. 所以,一元三值R_0函数共12个. 而一元三值函数共$3^{3^1}=27$个.

例2. 设$\bar{A}_0(x)=\neg(\neg x\rightarrow x)$,$\bar{A}_{\frac{1}{2}}(x)=(x\rightarrow\neg x)\wedge(\neg x\rightarrow x)$,$\bar{A}_1(x)=\neg(x\rightarrow\neg x)$,则在三值逻辑系统$L_3^*$中$\bar{A}_0(x)$,$\bar{A}_{\frac{1}{2}}(x)$,$\bar{A}_1(x)$的真值如表2所示.

表2 $\bar{A}_i(x)\left(i=0,\frac{1}{2},1\right)$的真值表

x	$\bar{A}_0(x)$	$\bar{A}_{\frac{1}{2}}(x)$	$\bar{A}_1(x)$
0	1	0	0
$\frac{1}{2}$	0	1	0
1	0	0	1

注7. 例2中给出的3个函数$\bar{A}_0(x)$,$\bar{A}_{\frac{1}{2}}(x)$,$\bar{A}_1(x)$均满足

$$\bar{A}_{\frac{k}{2}}(x)=\begin{cases}1, & x=\frac{k}{2}\\ 0, & x\neq\frac{k}{2}\end{cases},\ k=0,1,2.$$

下文中出现的$\bar{A}_0(x)$,$\bar{A}_{\frac{1}{2}}(x)$,$\bar{A}_1(x)$均为例2中定义的函数.

下面,我们依据Boole函数Shannon展开式的技巧,给出三值R_0函数的展开式.

命题5. 设$g(x_1,\cdots,x_n)$为n元三值R_0函数,则

$$g(x_1,x_2,\cdots,x_n)=(\bar{A}_0(x_1)\wedge g(0,x_2,\cdots,x_n))\vee\left(\bar{A}_{\frac{1}{2}}(x_1)\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\vee(\bar{A}_1(x_1)\wedge g(1,x_2,\cdots,x_n)).$$

证明.

$x_1=0$ 时，$(\overline{A}_0(x_1)\wedge g(0,x_2,\cdots,x_n))\vee\left(\overline{A}_{\frac{1}{2}}(x_1)\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\vee(\overline{A}_1(x_1)\wedge g(1,x_2,\cdots,x_n))=(1\wedge g(0,x_2,\cdots,x_n))\vee\left(0\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\vee(0\wedge g(1,x_2,\cdots,x_n))=g(0,x_2,\cdots,x_n)\vee 0\vee 0=g(0,x_2,\cdots,x_n)=g(x_1,x_2,\cdots,x_n)$；

$x_1=\frac{1}{2}$时，$(\overline{A}_0(x_1)\wedge g(0,x_2,\cdots,x_n))\vee\left(\overline{A}_{\frac{1}{2}}(x_1)\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\vee(\overline{A}_1(x_1)\wedge g(1,x_2,\cdots,x_n))=(0\wedge g(0,x_2,\cdots,x_n))\vee\left(1\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\vee(0\wedge g(1,x_2,\cdots,x_n))=0\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\vee 0=g\left(\frac{1}{2},x_2,\cdots,x_n\right)=g(x_1,x_2,\cdots,x_n)$；

$x_1=1$时，$(\overline{A}_0(x_1)\wedge g(0,x_2,\cdots,x_n))\vee\left(\overline{A}_{\frac{1}{2}}(x_1)\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\vee(\overline{A}_1(x_1)\wedge g(1,x_2,\cdots,x_n))=(0\wedge g(0,x_2,\cdots,x_n))\vee\left(0\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\vee(1\wedge g(1,x_2,\cdots,x_n))=0\vee 0\vee g(1,x_2,\cdots,x_n)=g(1,x_2,\cdots,x_n)=g(x_1,x_2,\cdots,x_n)$. 证毕.

命题 6. 设 $g(x_1,\cdots,x_n)$为 n 元三值 R_0 函数，约定 $x_k^0=\overline{A}_0(x_k)$，$x_k^{\frac{1}{2}}=\overline{A}_{\frac{1}{2}}(x_k)$，$x_k^1=\overline{A}_1(x_k)$（$k=1,2,$），则

$$g(x_1,x_2,x_3,\cdots,x_n)=\bigvee\left\{x_1^{\alpha_1}\wedge x_2^{\alpha_2}\wedge g(\alpha_1,\alpha_2,x_3,\cdots,x_n):(\alpha_1,\alpha_2)\in\left\{0,\frac{1}{2},1\right\}^2\right\}.$$

证明. 由命题 5 可知：

$$g(x_1,x_2,\cdots,x_n)=\bigvee\left\{x_1^{\alpha_1}\wedge g(\alpha_1,x_2,x_3,\cdots,x_n):\alpha_1\in\left\{0,\frac{1}{2},1\right\}\right\}\tag{3}$$

又

$$g(\alpha_1,x_2,x_3,\cdots,x_n)=\bigvee\left\{x_2^{\alpha_2}\wedge g(\alpha_1,\alpha_2,x_3,\cdots,x_n):\alpha_2\in\left\{0,\frac{1}{2},1\right\}\right\},\ \alpha_1=0,\frac{1}{2},1,$$

代入式(3)，整理得

$$g(x_1,x_2,x_3,\cdots,x_n)=\bigvee\left\{x_1^{\alpha_1}\wedge x_2^{\alpha_2}\wedge g(\alpha_1,\alpha_2,x_3,\cdots,x_n):(\alpha_1,\alpha_2)\in\left\{0,\frac{1}{2},1\right\}^2\right\}.$$ 证毕.

推论 3. 设 $g(x_1,\cdots,x_n)$为 n 元三值 R_0 函数，约定 $x_k^0=\overline{A}_0(x_k)$，$x_k^{\frac{1}{2}}=\overline{A}_{\frac{1}{2}}(x_k)$，$x_k^1=\overline{A}_1(x_k)$（$k=1,2,\cdots,n$），则

$$g(x_1,\cdots,x_n)=\bigvee\left\{x_1^{\alpha_1}\wedge\cdots\wedge x_n^{\alpha_n}\wedge g(\alpha_1,\cdots,\alpha_n):(\alpha_1,\cdots,\alpha_n)\in\left\{0,\frac{1}{2},1\right\}^n\right\}$$
$$=(\bigvee\{x_1^{\alpha_1}\wedge\cdots\wedge x_n^{\alpha_n}:(\alpha_1,\cdots,\alpha_n)\in g^{-1}(1)\})\vee\left(\bigvee\left\{x_1^{\alpha_1}\wedge\cdots\wedge x_n^{\alpha_n}\wedge\frac{1}{2}:(\alpha_1,\cdots,\alpha_n)\in g^{-1}\left(\frac{1}{2}\right)\right\}\right).$$

注 8.

(1)若$g^{-1}(1)=g^{-1}\left(\frac{1}{2}\right)=\varnothing$，即$g(x_1,\cdots,x_n)=0$. 这时可令 $g(x_1,\cdots,x_n)=x_1^0\wedge x_1^1$，即

$$g(x_1,\cdots,x_n)=\neg(\neg x_1\to x_1)\wedge\neg(x_1\to\neg x_1).$$

(2)若 $g^{-1}\left(\frac{1}{2}\right)\neq\varnothing$，则 $x_1,\cdots,x_n$ 中至少有一个取值$\frac{1}{2}$，则 $g(x_1,\cdots,x_n)$可表示为

$$(\bigvee\{x_1^{\alpha_1}\wedge\cdots\wedge x_n^{\alpha_n}:(\alpha_1,\cdots,\alpha_n)\in g^{-1}(1)\})\vee\left(\bigvee\left\{(x_1^{\alpha_1}\wedge(x_1\vee\neg x_1))\wedge\cdots\wedge(x_n^{\alpha_n}\wedge(x_n\vee\neg x_n)):(\alpha_1,\cdots,\alpha_n)\in g^{-1}\left(\frac{1}{2}\right)\right\}\right).$$

下面，给出命题 5、6 及推论 3 的对偶形式.

命题 7. 设 $g(x_1,\cdots,x_n)$为 n 元三值 R_0 函数，则

$$g(x_1,x_2,\cdots,x_n)=(\neg\overline{A}_0(x_1)\vee g(0,x_2,\cdots,x_n))\wedge\left(\neg\overline{A}_{\frac{1}{2}}(x_1)\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\wedge(\neg\overline{A}_1(x_1)\vee g(1,x_2,\cdots,x_n)).$$

证明.

$x_1=0$ 时，$(\neg\overline{A}_0(x_1)\vee g(0,x_2,\cdots,x_n))\wedge\left(\neg\overline{A}_{\frac{1}{2}}(x_1)\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\wedge(\neg\overline{A}_1(x_1)\vee g(1,x_2,\cdots,x_n))=(0\vee g(0,x_2,\cdots,x_n))\wedge\left(1\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\wedge(1\vee g(1,x_2,\cdots,x_n))=g(0,x_2,\cdots,x_n)\wedge 1\wedge 1=g(0,x_2,\cdots,x_n)=g(x_1,x_2,\cdots,x_n)$；

$x_1=\frac{1}{2}$时，$(\neg\overline{A}_0(x_1)\vee g(0,x_2,\cdots,x_n))\wedge\left(\neg\overline{A}_{\frac{1}{2}}(x_1)\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\wedge(\neg\overline{A}_1(x_1)\vee g(1,x_2,\cdots,x_n))=(1\vee g(0,x_2,\cdots,x_n))\wedge\left(0\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\wedge(1\vee g(1,x_2,\cdots,x_n))=1\wedge g\left(\frac{1}{2},x_2,\cdots,x_n\right)\wedge 1=g\left(\frac{1}{2},x_2,\cdots,x_n\right)=$

$g(x_1,x_2,\cdots,x_n)$；

$x_1=1$ 时，$(\neg\overline{A}_0(x_1)\vee g(0,x_2,\cdots,x_n))\wedge\left(\neg\overline{A}_{\frac{1}{2}}(x_1)\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\wedge(\neg\overline{A}_1(x_1)\vee g(1,x_2,\cdots,x_n))=(1\vee g(0,x_2,\cdots,x_n))\wedge\left(1\vee g\left(\frac{1}{2},x_2,\cdots,x_n\right)\right)\wedge(0\vee g(1,x_2,\cdots,x_n))=1\wedge 1\wedge g(1,x_2,\cdots,x_n)=g(1,x_2,\cdots,x_n)=g(x_1,x_2,\cdots,x_n)$.

证毕.

命题 8. 设 $g(x_1,\cdots,x_n)$ 为 n 元三值 R_0 函数，约定 $x_k^0=\neg\overline{A}_0(x_k)$，$x_k^{\frac{1}{2}}=\neg\overline{A}_{\frac{1}{2}}(x_k)$，$x_k^1=\neg\overline{A}_1(x_k)(k=1,2)$，则

$$g(x_1,x_2,x_3,\cdots,x_n)=\wedge\left\{x_1^{\beta_1}\vee x_2^{\beta_2}\vee g(\beta_1,\beta_2,x_3,\cdots,x_n):(\beta_1,\beta_2)\in\left\{0,\frac{1}{2},1\right\}^2\right\}.$$

证明. 由命题 7 可知：

$$g(x_1,x_2,\cdots,x_n)=\wedge\left\{x_1^{\beta_1}\vee g(\beta_1,x_2,x_3,\cdots,x_n):\beta_1\in\left\{0,\frac{1}{2},1\right\}\right\}\tag{4}$$

又

$$g(\beta_1,x_2,x_3,\cdots,x_n)=\wedge\left\{x_2^{\beta_2}\vee g(\beta_1,\beta_2,x_3,\cdots,x_n):\beta_2\in\left\{0,\frac{1}{2},1\right\}\right\},\ \beta_1=0,\frac{1}{2},1,$$

代入式(4)，整理得

$$g(x_1,x_2,x_3,\cdots,x_n)=\wedge\left\{x_1^{\beta_1}\vee x_2^{\beta_2}\vee g(\beta_1,\beta_2,x_3,\cdots,x_n):(\beta_1,\beta_2)\in\left\{0,\frac{1}{2},1\right\}^2\right\}.$$ 证毕.

推论 4. 设 $g(x_1,\cdots,x_n)$ 为 n 元三值 R_0 函数，约定 $x_k^0=\neg\overline{A}_0(x_k)$，$x_k^{\frac{1}{2}}=\neg\overline{A}_{\frac{1}{2}}(x_k)$，$x_k^1=\neg\overline{A}_1(x_k)$ $(k=1,2,\cdots,n)$，则

$$\begin{aligned}g(x_1,\cdots,x_n)&=\wedge\left\{x_1^{\beta_1}\vee\cdots\vee x_n^{\beta_n}\vee g(\beta_1,\cdots,\beta_n):(\beta_1,\cdots,\beta_n)\in\left\{0,\frac{1}{2},1\right\}^n\right\}\\&=(\wedge\{x_1^{\beta_1}\vee\cdots\vee x_n^{\beta_n}:(\beta_1,\cdots,\beta_n)\in g^{-1}(0)\})\wedge\\&\quad\left(\wedge\left\{x_1^{\beta_1}\vee\cdots\vee x_n^{\beta_n}\vee\frac{1}{2}:(\beta_1,\cdots,\beta_n)\in g^{-1}\left(\frac{1}{2}\right)\right\}\right).\end{aligned}$$

注 9.

(1) 若 $g^{-1}(0)=g^{-1}\left(\frac{1}{2}\right)=\varnothing$，即 $g(x_1,\cdots,x_n)=1$. 这时可令 $g(x_1,\cdots,x_n)=x_1^0\vee x_1^1$，即

$$g(x_1,\cdots,x_n)=(\neg x_1\to x_1)\vee(x_1\to\neg x_1).$$

(2) 若 $g^{-1}\left(\frac{1}{2}\right)\neq\varnothing$，则 $x_1,\cdots,x_n$ 中至少有一个取值 $\frac{1}{2}$，则 $g(x_1,\cdots,x_n)$ 可表示为

$$(\wedge\{x_1^{\beta_1}\vee\cdots\vee x_n^{\beta_n}:(\beta_1,\cdots,\beta_n)\in g^{-1}(0)\})\wedge\left(\wedge\left\{(x_1^{\beta_1}\vee(x_1\wedge\neg x_1))\vee\cdots\vee(x_n^{\beta_n}\vee(x_n\wedge\neg x_n)):(\beta_1,\cdots,\beta_n)\in g^{-1}\left(\frac{1}{2}\right)\right\}\right).$$

定理 1. n 元三值 R_0 函数 $g(x_1,\cdots,x_n)$ 共 $2^{2^n}\times 3^{3^n-2^n}$ 个.

证明. 因为 n 维向量 $(x_1,\cdots,x_n)\in\left\{0,\frac{1}{2},1\right\}^n$ 的不同选取共 3^n 个，其中 $x_1,\cdots,x_n$ 只取 0,1 两个值，不取 $\frac{1}{2}$ 的选取共 2^n 个；$x_1,\cdots,x_n$ 至少有一个取 $\frac{1}{2}$ 的选取共 3^n-2^n 个.

当 $x_1,\cdots,x_n$ 只取 0,1 两个值时，$g(x_1,\cdots,x_n)$ 的值只能为 0,1. 由推论 3 和注 8 可知，对 $x_1,\cdots,x_n$ 的 2^n 个选取 $g(x_1,\cdots,x_n)$ 都能取到 0 或 1 两个值.

当 $x_1,\cdots,x_n$ 至少有一个取 $\frac{1}{2}$ 时，由推论 3 和注 8 可知，对 $x_1,\cdots,x_n$ 的 3^n-2^n 个选取 $g(x_1,\cdots,x_n)$ 都能取到 0,1 或 $\frac{1}{2}$ 3 个值.

因此，n 元三值 R_0 函数 $g(x_1,\cdots,x_n)$ 共 $2^{2^n}\times 3^{3^n-2^n}$ 个. 证毕.

定义 11. 设 $A(p_1,\cdots,p_n)\in F(S)$，则分别当 A 具有形式

$(Q_{11}\wedge\cdots\wedge Q_{1m})\vee\cdots\vee(Q_{t1}\wedge\cdots\wedge Q_{tm})$ 或

$(Q_{11}\vee\cdots\vee Q_{1m})\wedge\cdots\wedge(Q_{t1}\vee\cdots\vee Q_{tm})$

时，称 A 为准析取范式或准合取范式，这里 $Q_{ij}=B(p_j)(j=1,\cdots,m;i=1,\cdots,t)$.

注 10.

(1) 在析取范式或合取范式中 Q_{ij} 取 p_j 或 $\neg p_j$；而在准析取范式或准合取范式中只要求 Q_{ij} 是含 p_j 的一元公式，如例 1 中的 $A_1=\neg(\neg p_1\to p_1)$，$B_1=\neg(p_1\to\neg p_1)$，$C_1=(p_1\to\neg p_1)\wedge(\neg p_1\to p_1)$，$C_1'=(p_1\to\neg p_1)\wedge(\neg p_1\to p_1)\wedge p_1$ 都可看作 Q_{i1}.

(2) 由 $B(p_j)$ 通过析(合)取连接词连接而成的公式叫简单准析(合)取式. 如 $B(p_1)\vee B(p_2)\vee B(p_3)$ 是简单准析取式，$B(p_1)\wedge B(p_2)$ 是简单准合取式. 简单准析(合)取式既可以看作是准析取范式，又可以看做准合取范式.

在三值逻辑系统 L_3^* 中，由逻辑公式 A 可以很

容易地得到 A 导出的三值 R_0 函数 $\overline{A}$. 反过来，由 n 元三值 R_0 函数 $g:\left\{0,\frac{1}{2},1\right\}^n\to\left\{0,\frac{1}{2},1\right\}$ 出发，如何构造一个 L_3^* 中的逻辑公式 A，使得 A 导出的三值 R_0 函数 $\overline{A}=g$ 呢？下面，我们解决这个问题.

例 3.　设 $g(x)$ 由表 3 给出，构造 L_3^* 中的一个逻辑公式 $A(p)$，使得 $A(p)$ 导出的三值 R_0 函数 $\overline{A}(x)=g(x)$.

表 3　$g(x)$ 的真值表

x	$g(x)$
0	0
$\frac{1}{2}$	$\frac{1}{2}$
1	0

解.　由注 8 中的第(2)条可知：$g(x)=\overline{A}_{\frac{1}{2}}(x)\wedge(x\vee\neg x)=(x\to\neg x)\wedge(\neg x\to x)\wedge(x\vee\neg x)$.

故，令 $A(p)=(p\to\neg p)\wedge(\neg p\to p)\wedge(p\vee\neg p)$，则 $A(p)$ 导出的三值 R_0 函数 $\overline{A}(x)=g(x)$.

例 4.　设 $g(x_1,x_2)$ 由表 4 给出，构造 L_3^* 中的一个逻辑公式 $A(p_1,p_2)$，使得 $A(p_1,p_2)$ 导出的三值 R_0 函数 $\overline{A}(x_1,x_2)=g(x_1,x_2)$.

表 4　$g(x_1,x_2)$ 的真值表

x_1	x_2	$g(x_1,x_2)$
0	0	1
0	$\frac{1}{2}$	0
0	1	1
$\frac{1}{2}$	0	1
$\frac{1}{2}$	$\frac{1}{2}$	1
$\frac{1}{2}$	1	$\frac{1}{2}$
1	0	0
1	$\frac{1}{2}$	$\frac{1}{2}$
1	1	1

解. 由注 9 中的第(2)条可知：$g(x_1,x_2)=(\neg\overline{A}_0(x_1)\vee\neg\overline{A}_{\frac{1}{2}}(x_2))\wedge((\neg\overline{A}_{\frac{1}{2}}(x_1)\vee(x_1\wedge\neg x_1))\vee\neg\overline{A}_1(x_2))\wedge(\neg\overline{A}_1(x_1)\vee\neg\overline{A}_0(x_2))\wedge(\neg\overline{A}_1(x_1)\vee(\neg\overline{A}_{\frac{1}{2}}(x_2)\vee(x_2\wedge\neg x_2)))$.

故，令 $A(p_1,p_2)=(\neg A_0(p_1)\vee\neg A_{\frac{1}{2}}(p_2))\wedge((\neg A_{\frac{1}{2}}(p_1)\vee(p_1\wedge\neg p_1))\vee\neg A_1(p_2))\wedge(\neg A_1(p_1)\vee\neg A_0(p_2))\wedge(\neg A_1(p_1)\vee(\neg A_{\frac{1}{2}}(p_2)\vee(p_2\wedge\neg p_2)))$，则 $A(p_1,p_2)$ 导出的三值 R_0 函数 $\overline{A}(x_1,x_2)=g(x_1,x_2)$.

这里 $A_0(p_i)=\neg(\neg p_i\to p_i)$，$A_{\frac{1}{2}}(p_i)=(p_i\to\neg p_i)\wedge(\neg p_i\to p_i)$，$A_1(p_i)=\neg(p_i\to\neg p_i)(i=1,2)$.

对于一般的 n 元三值 R_0 函数 $g(x_1,\cdots,x_n)$，我们有下面的定理.

定理 2.　任一 n 元三值 R_0 函数 $g(x_1,\cdots,x_n)$ 都可由某准析(合)取范式导出.

证明.　仅证合取范式的情形(析取范式的情形是类似的)

设 $g(x_1,\cdots,x_n)$ 为任意的 n 元三值 R_0 函数，约定 $p_k^0=\neg p_k\to p_k$，$p_k^{\frac{1}{2}}=\neg(p_k\to\neg p_k)\vee\neg(\neg p_k\to p_k)$，$p_k^1=p_k\to\neg p_k(k=1,2,\cdots,n)$，

(1) 当 $g^{-1}(0)=g^{-1}\left(\frac{1}{2}\right)=\varnothing$ 时，这时 $g(x_1,\cdots,x_n)=1$，令公式 $B(p_1)=(\neg p_1\to p_1)\vee(p_1\to\neg p_1)$，由注 9 可知，$B(p_1)$ 导出的函数就是 g，且 $B(p_1)$ 是简单准析取式，可以看做准合取范式.

(2) 当 $g^{-1}(0)\neq\varnothing$，$g^{-1}\left(\frac{1}{2}\right)=\varnothing$ 时，令公式 $A(p_1,\cdots,p_n)=\wedge\{p_1^{\beta_1}\vee\cdots\vee p_n^{\beta_n}:(\beta_1,\cdots,\beta_n)\in g^{-1}(0)\}$，由推论 4 可知，$A(p_1,\cdots,p_n)$ 导出的函数就是 g，且 $A(p_1,\cdots,p_n)$ 是准合取范式.

(3) 当 $g^{-1}\left(\frac{1}{2}\right)\neq\varnothing$ 时，这时 $x_1,\cdots,x_m$ 至少有一个取值 $\frac{1}{2}$，令公式 $A_1(p_1,\cdots,p_n)=(\wedge\{p_1^{\beta_1}\vee\cdots\vee p_n^{\beta_n}:(\beta_1,\cdots,\beta_n)\in g^{-1}(0)\})\wedge\left(\wedge\left\{(p_1^{\beta_1}\vee(p_1\wedge\neg p_1))\vee\cdots\vee(p_n^{\beta_n}\vee(p_n\wedge\neg p_n)):(\beta_1,\cdots,\beta_n)\in g^{-1}\left(\frac{1}{2}\right)\right\}\right)$，由注 9 可知，$A_1(p_1,\cdots,p_n)$ 导出的函数就是 g，且 $A_1(p_1,\cdots,p_n)$ 是准合取范式.

综上可知：任一 n 元三值 R_0 函数 $g(x_1,\cdots,x_n)$ 都可由某准析(合)取范式导出.　　证毕.

定理 3.　在 L_3^* 中，任一公式都逻辑等价于一个准析(合)取范式.

证明.　$\forall A\in F(S)$，不妨设 A 中含有 n 个原子命题 $p_1,\cdots,p_n$，则 A 导出一个 n 元三值 R_0 函数 $\overline{A}(x_1,\cdots,x_n)$. 由定理 2 知，$\overline{A}(x_1,\cdots,x_n)$ 可由准析(合)取范式 B 导出，且 $\overline{B}=\overline{A}(x_1,\cdots,x_n)$，所以 $A\approx B$.　　证毕.

定理 4.　在 L_3^* 中，n 元公式 $A(p_1,\cdots,p_n)$ 的逻辑等价类共 $2^{2^n}\times 3^{3^n-2^n}$ 个.

证明.　任意的 n 元三值 R_0 函数是由 n 元公式 $A(p_1,\cdots,p_n)$ 导出的，且任意的 n 元公式 $A(p_1,\cdots,p_n)$ 导出的函数也是 n 元三值 R_0 函数. 由定理 1 知，

n 元三值 R_0 函数 $g(x_1,\cdots,x_n)$ 共 $2^{2^n}\times 3^{3^n-2^n}$ 个. 由于逻辑等价的公式导出的三值 R_0 函数是相等的. 所以 n 元公式 $A(p_1,\cdots,p_n)$ 的逻辑等价类共 $2^{2^n}\times 3^{3^n-2^n}$ 个. 证毕.

4 L_3^* 中对称逻辑公式的计数问题及构造方法

定义 12[11]. 设 $g(x_1,\cdots,x_n)$ 是 n 元三值 R_0 函数,如果对 $(1,\cdots,n)$ 的任意置换 $(i_1,\cdots,i_n)$ 均有

$$g(x_{i_1},\cdots,x_{i_n})=g(x_1,\cdots,x_n),$$

则称 $g(x_1,\cdots,x_n)$ 为 n 元对称三值 R_0 函数.

命题 9[11]. 设 $\bar{g}:\left\{0,\frac{1}{2},1\right\}^n\to\left\{0,\frac{1}{2},1\right\}$ 为 n 元三值函数,如果 $\left\{0,\frac{1}{2},1\right\}^n$ 中的所有同类向量对应的函数值相等,则 $\bar{g}$ 为 n 元对称三值函数.

注 11. 同类向量的定义见文献[11]. 即设 $\boldsymbol{\alpha},\boldsymbol{\beta}$ 为 $\left\{0,\frac{1}{2},1\right\}^n$ 中的两个向量,如果 $\boldsymbol{\beta}$ 可由 $\boldsymbol{\alpha}$ 通过调整分量的次序而得到,则称 $\boldsymbol{\alpha},\boldsymbol{\beta}$ 为同类向量.

定理 5. n 元对称三值 R_0 函数 $g(x_1,\cdots,x_n)$ 共 $2^{n+1}\times 3^{\frac{n(n+1)}{2}}$ 个.

证明. 对于 n 维向量 $(x_1,\cdots,x_n)\in\left\{0,\frac{1}{2},1\right\}^n$,若 $x_1,\cdots,x_n$ 只取 0,1 两个值,则 n 维向量 $(x_1,\cdots,x_n)\in\{0,1\}^n$ 共有 $n+1$ 类同类向量. 这时,由推论 3 和注 8 可知,$g(x_1,\cdots,x_n)$ 的值只能取 0,1 两个值,且也能取到 0 或 1 两个值.

若 $x_1,\cdots,x_n$ 中只有 1 个取值 $\frac{1}{2}$,其余 $n-1$ 个只取 0,1 两个值,则 n 维向量 $(x_1,\cdots,x_n)\in\left\{0,\frac{1}{2},1\right\}^n$ 共有 n 类同类向量;若 $x_1,\cdots,x_n$ 中有 2 个取值 $\frac{1}{2}$,其余 $n-2$ 个只取 0,1 两个值,则 n 维向量 $(x_1,\cdots,x_n)\in\left\{0,\frac{1}{2},1\right\}^n$ 共有 $n-1$ 类同类向量;…;若 $x_1,\cdots,x_n$ 中有 $n-1$ 个取值 $\frac{1}{2}$,1 个只取 0,1 两个值,则 n 维向量 $(x_1,\cdots,x_n)\in\left\{0,\frac{1}{2},1\right\}^n$ 共有 2 类同类向量;若 $x_1,\cdots,x_n$ 中 n 个全取值 $\frac{1}{2}$,则 n 维向量 $(x_1,\cdots,x_n)\in\left\{0,\frac{1}{2},1\right\}^n$ 共有 1 类同类向量. 所以,$x_1,\cdots,x_n$ 中至少一个取值 $\frac{1}{2}$ 的共有 $1+2+\cdots+(n-1)+n=\frac{n(n+1)}{2}$ 类同类向量. 这时,由推论 3 和注 8 可知,$g(x_1,\cdots,x_n)$ 的值能取到 $0,\frac{1}{2},1$ 3 个值.

因此,n 元对称三值 R_0 函数 $g(x_1,\cdots,x_n)$ 共 $2^{n+1}\times 3^{\frac{n(n+1)}{2}}$ 个. 证毕.

定义 13[11]. 设 $A\in F(S)$,且 A 含有 n 个原子命题 $p_1,\cdots,p_n$. 如果 A 所诱导的三值 R_0 函数是对称三值 R_0 函数,则称 A 为 n 元对称逻辑公式.

例 5. 设 $A_k=\neg(\neg p_k\to p_k)$,$B_k=\neg(p_k\to\neg p_k)$,$C_k=(p_k\to\neg p_k)\wedge(\neg p_k\to p_k)$,$C_k'=C_k\wedge p_k$ $(k=1,2,3)$,令 $D_0=A_1\wedge A_2\wedge A_3$,$D_1=(B_1\wedge A_2\wedge A_3)\vee(A_1\wedge B_2\wedge A_3)\vee(A_1\wedge A_2\wedge B_3)$,$D_2=(B_1\wedge B_2\wedge A_3)\vee(B_1\wedge A_2\wedge B_3)\vee(B_1\wedge B_2\wedge A_3)$,$D_3=B_1\wedge B_2\wedge B_3$. 令 $E_{00}=C_1^*\wedge C_2^*\wedge C_3^*$;$E_{10}=(A_1\wedge C_2^*\wedge C_3^*)\vee(C_1^*\wedge A_2\wedge C_3^*)\vee(C_1^*\wedge C_2^*\wedge A_3)$,$E_{11}=(B_1\wedge C_2^*\wedge C_3^*)\vee(C_1^*\wedge B_2\wedge C_3^*)\vee(C_1^*\wedge C_2^*\wedge B_3)$;$E_{20}=(A_1\wedge A_2\wedge C_3^*)\vee(A_1\wedge C_2^*\wedge A_3)\vee(C_1^*\wedge A_2\wedge A_3)$,$E_{21}=(B_1\wedge A_2\wedge C_3^*)\vee(B_1\wedge C_2^*\wedge A_3)\vee(A_1\wedge B_2\wedge C_3^*)\vee(A_1\wedge C_2^*\wedge B_3)\vee(C_1^*\wedge B_2\wedge A_3)\vee(C_1^*\wedge A_2\wedge B_3)$,$E_{22}=(B_1\wedge B_2\wedge C_3^*)\vee(B_1\wedge C_2^*\wedge B_3)\vee(C_1^*\wedge B_2\wedge B_3)$. 这里,每一个 E_k $(k\in N_1=\{00\}\cup\{10,11\}\cup\{20,21,22\})$ 中的 C_l^* $(l=1,2,3)$ 或者全部取 C_l 或者全部取 C_l'. 显然,逻辑公式 $D_0,D_1,D_2,D_3,E_{00},E_{10},E_{11},E_{20},E_{21},E_{22}$ 均为 L_3^* 中的 3 元对称逻辑公式. 再令 $\Gamma=\{(\bigvee_{j\in J}D_j)\vee(\bigvee_{k\in K}E_k)\mid J$ 是集合 $M_1=\{0,1,2,3\}$ 的任意子集,K 是集合 N_1 的任意子集$\}$,当 $J=K=\varnothing$ 时,规定 $(\bigvee_{j\in\phi}D_j)\vee(\bigvee_{k\in\phi}E_k)=\neg((\bigvee_{j\in M_1}D_j)\vee(\bigvee_{k\in N_1}E_k))$,则 Γ 中的所有公式均为 L_3^* 中的 3 元对称逻辑公式.

例 6. 设 $A_k=\neg(\neg p_k\to{}_k)$,$B_k=\neg(p_k\to\neg p_k)$,$C_k=(p_k\to\neg p_k)\wedge(\neg p_k\to p_k)$,$C_k'=C_k\wedge p_k$ $(k=1,2,\cdots,n)$,令 $D_0=\vee\{A_{i_1}\wedge A_{i_2}\wedge\cdots\wedge A_{i_n}\mid(i_1,i_2,\cdots,i_n)$ 是 $(1,2,\cdots,n)$ 的任意置换$\}$,$D_1=\vee\{B_{i_1}\wedge A_{i_2}\wedge\cdots\wedge A_{i_n}\mid(i_1,i_2,\cdots,i_n)$ 是 $(1,2,\cdots,n)$ 的任意置换$\}$,$D_2=\vee\{B_{i_1}\wedge B_{i_2}\wedge\cdots\wedge A_{i_n}\mid(i_1,i_2,\cdots,i_n)$ 是 $(1,2,\cdots,n)$ 的任意置换$\}$,…,$D_{n-1}=\vee\{B_{i_1}\wedge B_{i_2}\wedge\cdots\wedge B_{i_{n-1}}\wedge A_{i_n}\mid(i_1,i_2,\cdots,i_{n-1},i_n)$ 是 $(1,2,\cdots,n-1,n)$ 的任意置换$\}$,$D_n=\vee\{B_{i_1}\wedge B_{i_2}\wedge\cdots\wedge B_{i_n}\mid(i_1,i_2,\cdots,i_n)$ 是 $(1,2,\cdots,n)$ 的任意置换$\}$. 令 $E_{00}=\vee\{C_{i_1}^*\wedge C_{i_2}^*\wedge\cdots\wedge C_{i_n}^*\mid(i_1,i_2,\cdots,i_n)$ 是 $(1,2,\cdots,n)$ 的任意置换$\}$;$E_{10}=$

$\vee\{A_{i_1}\wedge C_{i_2}^*\wedge\cdots\wedge C_{i_n}^*\mid(i_1,i_2,\cdots,i_n)$是$(1,2,\cdots,n)$的任意置换$\}$，$E_{11}=\vee\{B_{i_1}\wedge C_{i_2}^*\wedge\cdots\wedge C_{i_n}^*\mid(i_1,i_2,\cdots,i_n)$是$(1,2,\cdots,n)$的任意置换$\}$；$E_{20}=\vee\{A_{i_1}\wedge A_{i_2}\wedge C_{i_3}^*\wedge\cdots\wedge C_{i_n}^*\mid(i_1,i_2,i_3,\cdots,i_n)$是$(1,2,3,\cdots,n)$的任意置换$\}$，$E_{21}=\vee\{B_{i_1}\wedge A_{i_2}\wedge C_{i_3}^*\wedge\cdots\wedge C_{i_n}^*\mid(i_1,i_2,i_3,\cdots,i_n)$是$(1,2,3,\cdots,n)$的任意置换$\}$，$E_{22}=\vee\{B_{i_1}\wedge B_{i_2}\wedge C_{i_3}^*\wedge\cdots\wedge C_{i_n}^*\mid(i_1,i_2,i_3,\cdots,i_n)$是$(1,2,3,\cdots,n)$的任意置换$\}$；…；$E_{(n-1)0}=\vee\{A_{i_1}\wedge A_{i_2}\wedge\cdots\wedge A_{i_{n-1}}\wedge C_{i_n}^*\mid(i_1,i_2,\cdots,i_{n-1},i_n)$是$(1,2,\cdots,n-1,n)$的任意置换$\}$，$E_{(n-1)1}=\vee\{B_{i_1}\wedge A_{i_2}\wedge\cdots\wedge A_{i_{n-1}}\wedge C_{i_n}^*\mid(i_1,i_2,\cdots,i_{n-1},i_n)$是$(1,2,\cdots,n-1,n)$的任意置换$\}$，$E_{(n-1)2}=\vee\{B_{i_1}\wedge B_{i_2}\wedge A_{i_3}\wedge\cdots\wedge A_{i_{n-1}}\wedge C_{i_n}^*\mid(i_1,i_2,i_3,\cdots,i_{n-1},i_n)$是$(1,2,3,\cdots,n-1,n)$的任意置换$\}$，…，$E_{(n-1)(n-1)}=\vee\{B_{i_1}\wedge B_{i_2}\wedge\cdots\wedge B_{i_{n-1}}\wedge C_{i_n}^*\mid(i_1,i_2,\cdots,i_{n-1},i_n)$是$(1,2,\cdots,n-1,n)$的任意置换$\}$. 这里，每一个 $E_k(k\in N=\{00\}\cup\{10,11\}\cup\{20,21,22\}\cup\cdots\cup\{(n-1)0,(n-1)1,(n-1)2,\cdots,(n-1)(n-1)\})$中的 $C_l^*(l=1,2,\cdots,n)$或者全部取C_l或者全部取 C'_l. 显然，逻辑公式 $D_j,E_k(j\in M=\{0,1,2,\cdots,n\},k\in N)$均为 L_3^* 中的 n 元对称逻辑公式. 再令 $\Gamma=\{(\bigvee\limits_{j\in J}D_j)\vee(\bigvee\limits_{k\in K}E_k)\mid J$是集合 M 的任意子集，K 是集合 N 的任意子集$\}$，当 $J=K=\varnothing$时，规定$(\bigvee\limits_{j\in\varphi}D_j)\vee(\bigvee\limits_{k\in\varphi}E_k)=\neg((\bigvee\limits_{j\in M}D_j)\vee(\bigvee\limits_{k\in N}E_k))$，则 Γ 中的所有公式均为 L_3^* 中的 n 元对称逻辑公式.

注 12. 在例 6 中逻辑公式$D_j,E_k(j\in M,k\in N)$的形式是可以化简的，例如D_0可化简为$A_0\wedge A_1\wedge\cdots\wedge A_n$，$D_1$可化简为$(B_1\wedge A_2\wedge\cdots\wedge A_{n-1}\wedge A_n)\vee(A_1\wedge B_2\wedge\cdots\wedge A_{n-1}\wedge A_n)\vee\cdots\vee(A_1\wedge A_2\wedge\cdots\wedge B_{n-1}\wedge A_n)\vee(A_1\wedge A_2\wedge\cdots\wedge A_{n-1}\wedge B_n)$，$E_0$可化简为 $E_0=C_1^*\wedge C_2^*\wedge\cdots\wedge C_n^*$.

命题 10. 设 Γ 的定义同例 6，则 Γ 中含有$2^{n+1}\times 3^{\frac{n(n+1)}{2}}$个 n 元对称逻辑公式.

证明. 因为 $M=\{0,1,2,\cdots,n\}$的所有子集共2^{n+1}个，所以$\bigvee\limits_{j\in J}\{D_j\mid J$是集合 M 的任意子集$\}$中公式的不同组合方式有 2^{n+1}个.

在$\bigvee\limits_{k\in K}\{E_k\mid K$是集合 N 的任意子集$\}$中，由于集合 N 中共有 $1+2+\cdots+n=\frac{n(n+1)}{2}$个元素，且每一个 $E_k(k\in N)$中的 $C_k^*(k=1,2,\cdots,n)$或者全部取 C_k 或者全部取 C'_k，所以 $K=\varnothing$时，对应 1 个公式；K 中含有 1 个元素时，对应 $\begin{pmatrix}1\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2$ 个公式；K 中含有 2 个元素时，对应 $\begin{pmatrix}2\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2^2$ 个公式；…；K 中含有 i 个元素时，对应 $\begin{pmatrix}i\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2^i$ 个公式；…；K 中含有$\frac{n(n+1)}{2}$个元素时，对应 $\begin{pmatrix}\frac{n(n+1)}{2}\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2^{\frac{n(n+1)}{2}}$ 个公式. 从而可得$\bigvee\limits_{k\in K}\{E_k\mid K$ 是集合 N 的任意子集$\}$中公式的不同组合方式有

$$1+\begin{pmatrix}1\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2+\begin{pmatrix}2\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2^2+\cdots+\begin{pmatrix}i\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2^i+\cdots+\begin{pmatrix}\frac{n(n+1)}{2}\\ \frac{n(n+1)}{2}\end{pmatrix}\times 2^{\frac{n(n+1)}{2}}=(1+2)^{\frac{n(n+1)}{2}}=3^{\frac{n(n+1)}{2}}\text{个}.$$

因此，Γ 中含有 $2^{n+1}\times 3^{\frac{n(n+1)}{2}}$ 个 n 元对称逻辑公式. 证毕.

命题 11. 设逻辑公式$D_j,E_k(j\in M,k\in N)$的定义同例 6，$\forall i\in\{0,1,2,\cdots,n\}$，对于赋值 $v(p_1)=\cdots=v(p_i)=0,v(p_{i+1})=\cdots=v(p_n)=1$，均有 $v(D_j)=\begin{cases}1, & j=i\\ 0, & j\neq i\end{cases}(j\in M)$，$v(E_k)=0(k\in N)$. $\forall i_1\leq i_2\in\{1,2,\cdots,n\}$，对于赋值 $v(p_1)=\cdots=v(p_{i_1})=\frac{1}{2}$，$v(p_{i_1+1})=\cdots=v(p_{i_2})=1,v(p_{i_2+1})=\cdots=v(p_n)=0$，均有 $v(D_j)=0(j\in M)$，

$$v(E_{st})=\begin{cases}1, & s=n-i_1,t=i_2-i_1,C_l^*(l=1,2,\cdots,n)\text{全部取}C_l\\ \frac{1}{2}, & s=n-i_1,t=i_2-i_1,C_l^*(l=1,2,\cdots,n)\text{全部取}C'_l.\\ 0, & \text{其它}\end{cases}$$

证明. $\forall i\in\{0,1,2,\cdots,n\}$，对于赋值$v(p_1)=\cdots=v(p_i)=0,v(p_{i+1})=\cdots=v(p_n)=1$，有$v(A_1)=\cdots=v(A_i)=1,v(B_1)=\cdots=v(B_i)=0$；$v(A_{i+1})=\cdots=v(A_n)=0,v(B_{i+1})=\cdots=v(B_n)=0$，所以 $v(D_j)=\begin{cases}1, & j=i\\ 0, & j\neq i\end{cases}(j\in M)$. 这时，$v(C_1)=\cdots=v(C_n)=0$，$v(C'_1)=\cdots=v(C'_n)=0$，从而 $v(C_1^*)=\cdots=v(C_n^*)=0$，所以 $v(E_k)=0(k\in N)$.

$\forall i_1\leq i_2\in\{1,2,\cdots,n\}$，对于赋值 $v(p_1)=\cdots=v(p_{i_1})=\frac{1}{2},v(p_{i_1+1})=\cdots=v(p_{i_2})=1,v(p_{i_2+1})=\cdots=$

$v(p_n)=0$,有 $v(A_1)=\cdots=v(A_{i_1})=0,v(B_1)=\cdots=v(B_{i_1})=0$,所以$v(D_j)=0(j\in M)$. 而$v(A_{i_1+1})=\cdots=v(A_{i_2})=0,v(B_{i_1+1})=\cdots=v(B_{i_2})=1$;$v(A_{i_2+1})=\cdots=v(A_n)=1,v(B_{i_2+1})=\cdots=v(B_n)=0$;$v(C_1)=\cdots=v(C_{i_1})=1,v(C'_1)=\cdots=v(C'_{i_1})=\frac{1}{2},v(C^*_{i_1+1})=\cdots=v(C^*_n)=0$,所以

$$v(E_{st})=\begin{cases}1, & s=n-i_1,t=i_2-i_1,C^*_l(l=1,2,\cdots,n)\text{全部取}C_l\\ \frac{1}{2}, & s=n-i_1,t=i_2-i_1,C^*_l(l=1,2,\cdots,n)\text{全部取}C'_l.\\ 0, & \text{其它}\end{cases}$$

证毕.

命题 12. 设Γ的定义同例 6,则Γ中的逻辑公式导出的 n 元三值 R_0 函数是两两互异的.

证明. 设 A,B 是 Γ 中的任意两个公式,则存在 $J_1,J_2\subseteq M,K_1,K_2\subseteq N$,使得 $A=(\bigvee_{j\in J_1}D_j)\vee(\bigvee_{k\in K_1}E_k),B=(\bigvee_{j\in J_2}D_j)\vee(\bigvee_{k\in K_2}E_k)$. 因为 A,B 是 Γ 中的两个不同的公式,所以 $J_1\neq J_2$或者 $K_1\neq K_2$或者 $J_1=J_2,K_1=K_2$,但存在 $m\in K_1=K_2$,使得 E_m中的 $C^*_l(l=1,2,\cdots,n)$的取法不同.

(1) 若 $J_1\neq J_2$,则存在 $i\in M$,使得 $i\in J_1$但 $i\notin J_2$(或 $i\in J_2$但 $i\notin J_1$),不妨设是前一种情形,即 $i\in J_1$但 $i\notin J_2$,则对于赋值 $v(p_1)=\cdots=v(p_i)=0$,$v(p_{i+1})=\cdots=v(p_n)=1$,有 $v(D_j)=\begin{cases}1, & j=i\\ 0, & j\neq i\end{cases}(j\in M)$;$v(E_k)=0(k\in N)$. 从而有 $v(A)=1,v(B)=0$,即 A,B 诱导的 n 元三值 R_0 函数是互异的.

(2) 若 $K_1\neq K_2$,则存在 $i\in M$,使得 $i\in K_1$但 $i\notin K_2$(或 $i\in K_2$但 $i\notin K_1$),不妨设是前一种情形,即 $i\in K_1$但 $i\notin K_2$. 这时,设 $i=st(t\leq s)$,记 $i_1=n-s$,$i_2=i_1+t$,则对于赋值 $v(p_1)=\cdots=v(p_{i_1})=\frac{1}{2}$,$v(p_{i_1+1})=\cdots=v(p_{i_2})=1,v(p_{i_2+1})=\cdots=v(p_n)=0$,有 $v(D_j)=0(j\in M)$; $v(E_i)=v(E_{st})=1$ 或$\frac{1}{2}$,$v(E_k)=0(k\neq i,k\in N)$. 从而有 $v(A)=1$ 或$\frac{1}{2}$,$v(B)=0$,即 A,B 诱导的 n 元三值 R_0 函数是互异的.

(3) 若 $J_1=J_2,K_1=K_2$且存在 $i=st\in K_1=K_2$ $(t\leq s)$满足 A 中的 E_{st} 中的 C^*_j 全取 C_j,而 B 中的 E_{st} 中的 C^*_j 全取 C'_j(或 A 中的 E_{st} 中的 C^*_j 全取C'_j,而 B 中的 E_{st} 中的 C^*_j 全取 C_j)$(j=1,2,\cdots,n)$. 不妨设是前一种情形,记 $i_1=n-s,i_2=i_1+t$,则对于赋值 $v(p_1)=\cdots=v(p_{i_1})=\frac{1}{2},v(p_{i_1+1})=\cdots=v(p_{i_2})=1,v(p_{i_2+1})=\cdots=v(p_n)=0$,有 $v(D_j)=0$ $(j\in M)$;$v(E_k)=0(k\neq i,k\in N)$. 当 E_i中的 C^*_j 全取 C_j时,$v(E_i)=1$; 当 E_i中的 C^*_j 全取C'_j时,$v(E_i)=\frac{1}{2}$. 所以 $v(A)=1,v(B)=\frac{1}{2}$,即 A,B 诱导的n 元三值 R_0 函数是互异的. 证毕.

定理 6. 设 $A\in F(S)$,且 A 中含有 n 个原子命题 $p_1,\cdots,p_n$,Γ 的定义同例 6. 若 A 是逻辑系统 L^*_3 中的对称逻辑公式,则存在逻辑公式 $B\in\Gamma$,使得 $A\approx B$.

证明. 因为 A 中含有 n 个原子命题 $p_1,\cdots,p_n$,且是 L^*_3 中的对称逻辑公式,所以 A 诱导的三值 R_0函数是 n 元对称三值 R_0 函数,而由命题 10 知,集合 $\Gamma=\{(\bigvee_{j\in J}D_j)\vee(\bigvee_{k\in K}E_k)\mid J\text{是集合}M\text{的任意子集},K\text{是集合}N\text{的任意子集}\}$中共有 $2^{n+1}\times3^{\frac{n(n+1)}{2}}$ 个 n 元对称逻辑公式. 由命题 12 知,这些对称逻辑公式诱导的 $2^{n+1}\times3^{\frac{n(n+1)}{2}}$ 个 n 元对称三值 R_0 函数是两两互异的,再由定理 5 知,n 元对称三值 R_0 函数共有 $2^{n+1}\times3^{\frac{n(n+1)}{2}}$ 个. 所以存在逻辑公式 $B\in\Gamma$,使得 B 与 A 诱导的 n 元对称三值 R_0 函数相同,即 $A\approx B$. 证毕.

注 13. 定理 6 给出了三值逻辑系统 L^*_3 中对称逻辑公式的构造方法,在逻辑等价的意义下,例 6 中的公式集 Γ 给出了 L^*_3 中全部的 $2^{n+1}\times3^{\frac{n(n+1)}{2}}$ 个 n 元对称逻辑公式.

5 结束语

本文由 Boole 函数 Shannon 的展开式出发,研究了三值 R_0 函数的展开式,得到了三值 R_0 函数的构造方法,解决了其计数问题. 在此基础上,研究了三值逻辑系统 L^*_3 中逻辑公式的计数问题,给出了逻辑公式的准析取范式和准合取范式表示,并给出了对称逻辑公式的构造方法. 而对于一般的 n 值 R_0 函数(例如四值、五值)的展开式以及计数问题还没有解决,这是一个值得继续研究的课题.

参 考 文 献

[1] Baier C, Katoen J-P. Principles of Model Checking. London, UK: The MIT Press Cambridge, 2008

[2] Dasgupta P, Chakrabarti P P, Deka J K, Sankaranarayanan S. Min-max computation tree logic. Artificial Intelligence, 2001, 127(1): 137-162

[3] Ivančić F, Yang Z J, Ganai M K, Gupta A, Ashar P. Efficient SAT-based bounded model checking for software verification. Theoretical Computer Science, 2008, 404(3): 256-274

[4] Basagiannis S, Katsaros P, Pombortsis A. An intruder model with message inspection for model checking security protocols. Computer & Security, 2010, 29(1): 16-34

[5] Burkart O, Steffen B. Model checking the full modal mu-calculus for infinite sequential processes. Theoretical Computer Science,1999, 221(1-2): 251-270

[6] Qian Jun-Yan, Xu Bao-Wen. Model checking CTL based on complete abstraction interpretation. Chinese Journal of Computers, 2009, 32(5): 992-1001(in Chinese)
(钱俊彦，徐宝文. 基于完备抽象解释的模型检验 CTL 公式研究. 计算机学报，2009，32(5)：992-1001)

[7] Raimondi F, Lomuscio A. Automatic verification of multi-agent systems by model checking via ordered binary decision diagrams. Journal of Applied Logic, 2007, 5(2): 235-251

[8] Wen Qiao-Yan, Niu Xin-Xin, Yang Yi-Xian. Boolean Function in Modern Cryptology. Beijing: Science Press, 2000(in Chinese)
(温巧燕，钮心忻，杨义先. 现代密码学中的布尔函数. 北京：科学出版社，2000)

[9] Stănică Pantelimon, Maitra Subhamoy. Rotation symmetric Boolean functions — Count and cryptographic properties. Discrete Applied Mathematics, 2008, 156(10): 1567-1580

[10] Sarkar Palash, Maitra Subhamoy. Balancedness and correlation immunity of symmetric Boolean functions. Discrete Mathematics, 2007, 307(19-20): 2351-2358

[11] Wang Qing-Ping, Wang Guo-Jun. Distribution of the symmetrical logic formulas in the L_3^*-logic metric space. Chinese Journal of Computers, 2011, 34(1): 105-114(in Chinese)
(王庆平，王国俊. 对称逻辑公式在 L_3^* 逻辑度量空间中的分布. 计算机学报，2011，34(1)：105-114)

[12] Wang Guo-Jun, Zhou Hong-Jun. Introduction to Mathematical Logic and Resolution Principle. 2nd Edition. Beijing: Science Press; Oxford, U. K.: Alpha Science International Limited, 2009

WANG Qing-Ping, born in 1979, Ph. D. candidate, lecturer. His research interests include fuzzy logic, uncertain reasoning etc.

Background

In recent years, the technique of model checking has been developed rapidly and this technique has been applied in various fields such as aerospace, e-commerce, communication technology and medical system successfully. Model checking is an automatic formal verification technique for verifying a transition system whether satisfies the predetermined specification. In order to simplify the verification process, the symbolic model checking was proposed in computing tree logic[1]. In order to symbolize states and the transition relationships of states, switching functions and Shannon expansion of Boole function were given.

The concept of three valued R_0 function was given by authors in 2011 and the symmetric logic formulae are studied. In this paper, Shannon expansion of Boole function in symbolic computation tree logic is generalized. In three-valued logic system L_3^*, the expansions of symmetric three-valued R_0 function which are induced by logical formulae are studied, and the quasi disjunctive normal form and quasi conjunctive normal form of logical formulae are given. The counting problems of n-ary three-valued R_0 functions and n-ary logical formulae are studied. Then the construction method of symmetrical logic formulae in L_3^* is given.

This work is supported by the National Natural Science Foundation of China under Grant Nos. 11171200, 61005046, 61103133 and the Doctoral Program of Higher Education Special Research of Ministry of Education under Grant No. 20100202120012.